UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,634	04/13/2001	M. Paul Zavidniak	026590-006	3065

7590	07/11/2005

Richard J. McGrath
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

EXAMINER
MILLER, BRANDON J

ART UNIT	PAPER NUMBER
2683	

DATE MAILED: 07/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/833,634	ZAVIDNIAK, M. PAUL
	Examiner	Art Unit	
	Brandon J. Miller	2683	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *17 March 2005*.

2a) ☐ This action is **FINAL**.　　2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-24* is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☒ Claim(s) *14 and 15* is/are allowed.

6) ☒ Claim(s) *1-3,10-13,16-19 and 21-23* is/are rejected.

7) ☐ Claim(s) *4-9,20 and 24* is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a) ☐ All　b) ☐ Some *　c) ☐ None of:

　　　1. ☐ Certified copies of the priority documents have been received.

　　　2. ☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Allowable Subject Matter

Claims 14-15 are allowed. Claim 14 is allowable because the prior art does not teach or

fairly suggest the claim limitation " A method of detecting intrusions in the Tactical Internet".

Claim 15 is allowable because the prior art does not teach or fairly suggest the claim limitation "

A method of detecting intrusions in a RF based tactical data link".

Claims 4-9, 20 and 24 are objected to as being dependent upon a rejected base claim, but

would be allowable if rewritten in independent form including all of the limitations of the base

claim and any intervening claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 10-13, 16-19, and 21-23 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Huff view of Ko.

Regarding claim 1 Huff teaches a method of detecting intrusions in a wireless network

(see col. 13, lines 44-49 and col. 14, lines 16-20). Huff teaches researching and defining normal

network behavior with the intent of ascertaining user and temporal patterns (see col. 10, lines 27-

28 & 32-37). Huff teaches researching potential sources of information that will lead to the

detection and classification of potentially intrusive events (see col. 10, lines 54-56). Huff

teaches establishing a knowledge base of anomalous network activity that will form the

foundation for classifying potentially intrusive events (see col. 7, lines 52-57). Huff teaches

analyzing and evaluating a knowledge base to dispatch countermeasure agents; and utilizing the

countermeasure agents to provide an adaptive response to intrusions in the network (see col. 10,

lines 54-67 and col. 11, line 1). Huff does not specifically teach creating an attack model. Ko

teaches analyzing and evaluating a knowledge base to create an attack model (see col. 5, lines

20-25 and col. 7, lines 34-39). Ko teaches utilizing the attack model to provide an adaptive

response to intrusions in the wireless network (see col. 5, lines 26-28 and col. 7, lines 34-39). It

would have been obvious to one of ordinary skill in the art at the time the invention was made to

modify the countermeasure in Huff to include creating an attack model because this would allow

for an alternative device that detects and prevents unauthorized network access.

Regarding claim 2 Huff teaches collecting real-world information concerning potentially

intrusive events and updating the knowledge base (see col. 7, lines 52-55).

Regarding claim 3 Huff teaches developing a recovery model to recover from an

intrusion of the network (see col. 10, lines 61-67 and col. 11, line 1).

Regarding claim 10 Huff teaches data related to suspicious events including passive

eavesdropping, deception and denial of service (see col. 7, lines 52-55 and col. 12, lines 25-34).

Regarding claim 11 Ko teaches an attack model that is utilized to generate signatures of

suspicious events (see col. 6, lines 1-4 and col. 8, lines 54-55).

Regarding claim 12 Ko teaches an attack model that is utilized to generate recommendations regarding the set up of a network (see col. 5, lines 20-25 and col. 6, lines 21-24).

Regarding claim 13 Huff teaches a method of detecting intrusions in a wireless network (see col. 13, lines 44-49 and col. 14, lines 16-20). Huff teaches researching and defining normal network behavior with the intent of ascertaining user and temporal patterns (see col. 10, lines 27-28 & 32-37). Huff teaches researching potential sources of information that will lead to the detection and classification of potentially intrusive events (see col. 10, lines 54-56). Huff teaches augmenting the researching step by collecting real-world information concerning intrusive events and updating the knowledge base (see col. 7, lines 52-54). Huff teaches establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events (see col. 7, lines 52-57). Huff teaches analyzing and evaluating a knowledge base to dispatch countermeasure agents; and utilizing the countermeasure agents to provide an adaptive response to intrusions in the network (see col. 10, lines 54-67 and col. 11, line 1). Huff teaches developing a recovery model to recover from an intrusion of the network (see col. 10, lines 61-67 and col. 11, line 1). Huff does not specifically teach creating an attack model. Ko teaches analyzing and evaluating a knowledge base to create an attack model (see col. 5, lines 20-25 and col. 7, lines 34-39). Ko teaches utilizing the attack model to provide an adaptive response to intrusions in the wireless network (see col. 5, lines 26-28 and col. 7, lines 34-39). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the countermeasure in Huff to include creating an attack

model because this would allow for an alternative device that detects and prevents unauthorized network access.

Regarding claim 16 Ko teaches an attack model that comprises an identification of a plurality of types of hostile events and associated manifestations of anomalous network events (see col. 5, lines 20-25 and col. 7, lines 34-39).

Regarding claim 17 Ko teaches generating signatures from an attack model (see col. 6, lines 1-4 and col. 8, lines 54-55).

Regarding claim 18 Huff teaches a wireless network that is an RF radio communication system (see col. 13, lines 44-16 & 54-57).

Regarding claim 19 Ko teaches anomalous network activity that includes network performance data (see col. 7, lines 1-3).

Regarding claim 21 Huff teaches a method of detecting intrusions in a RF-based radio communication system (see col. 13, lines 44-49 & 55-57 and col. 14, lines 16-20). Huff teaches establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events, wherein the knowledge base includes data relating to suspicious events including passive eavesdropping, deception and denial of service (see col. 7, lines 52-57 and col. 12, lines 25-34). Huff teaches analyzing and evaluating a knowledge base to create countermeasure agents; and utilizing the countermeasure agents to provide an adaptive response to intrusions in the network (see col. 10, lines 54-67, col. 11, line 1, and col. 14, lines 40-42). Huff teaches developing a recovery model to recover from an intrusion on the network (see col. 10, lines 61-67 and col. 11, line 1). Huff does not specifically teach creating an attack model that comprises an identification of a plurality of types of hostile events and associated

manifestations of anomalous network events. Ko teaches analyzing and evaluating a knowledge base to create an attack model that comprises an identification of a plurality of types of hostile events and associated manifestations of anomalous network events (see col. 5, lines 20-25 and col. 7, lines 34-39). Ko teaches utilizing the attack model to provide an adaptive response to intrusions in the wireless network (see col. 5, lines 26-28 and col. 7, lines 34-39). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention to include detecting intrusions in the Tactical Internet and creating an attack model because this would allow for an alternative device that detects and prevents unauthorized Internet access.

Regarding claim 22 Ko teaches a device as recited in claim 17 and is rejected given the same reasoning as reasoning as above.

Regarding claim 23 Ko teaches a device as recited in claim 19 and is rejected given the same reasoning as reasoning as above.

Response to Arguments

Applicant's arguments with respect to claims 1-3, 10, and 13, 16-19, and 21-23 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Sawyer U.S Patent No. 6,073,006 discloses a method and apparatus for detecting and preventing fraud in a satellite communication system.

Ferrel U.S Patent No. 5,005,210 discloses a method and apparatus for characterizing a radio transmitter.

Martin U.S Patent No. 6,772,349 B1 discloses detection of an attack such as a pre-attack on a computer network.

Porras U.S Patent No. 6,321,338 discloses network surveillance.

Froutan U.S Patent No. 6,654,882 discloses a network security system protecting against disclosure of information to unauthorized agents.

Sabatino U.S Patent No. 6,765,498 B1 discloses an embedded digitization system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon J. Miller whose telephone number is 571-272-7869. The examiner can normally be reached on Mon.-Fri. 8:00 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Trost can be reached on 571-272-7872. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

June 13, 2005

WILLIAM TROST
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600